Кушнир Светлана Ивановна
канд. ист. наук, доцент, доцент
ФКОУ ВО «Воронежский институт Федеральной
службы исполнения наказаний»
г. Воронеж, Воронежская область
Кушнир Михаил Станиславович
студент
ФГБОУ ВО «Воронежский государственный
университет инженерных технологий»
г. Воронеж, Воронежская область

ШИФРОВАНИЕ И ЗАЩИТА ОТ DDOS-АТАК, КАК ОДНИ ИЗ КОМПОНЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация*: информационная безопасность является одним из основных аспектов общей безопасности в современном информационном обществе. Компонентами информационной безопасности являются конфиденциальность, целостность, доступность, аутентификация и авторизация, защита от вредоносных программ, аудит и мониторинг и даже физическая безопасность.*

Ключевые слова*: информационная безопасность, конфиденциальность, аутентификация, авторизация, вредоносные программы, шифрование, DdoS-атаки, мониторинг.*

Информационная безопасность (или ИБ) – это область, которая занимается защитой информации от различных угроз и рисков, таких как несанкционированный доступ, разрушение, утечка или модификация данных. Информация, которую нужно защищать, может включать в себя данные организации, личные данные клиентов, государственные секреты, финансовую информацию и многое другое.

Важные аспекты информационной безопасности включают:

Конфиденциальность: обеспечение конфиденциальности данных, то есть предотвращение несанкционированного доступа к ним.

Целостность: гарантирование целостности данных, чтобы они не были повреждены или изменены без разрешения.

Доступность: обеспечение доступности данных и информационных ресурсов в нужное время для авторизованных пользователей.

Аутентификация и авторизация: подтверждение личности пользователей (аутентификация) и управление их правами доступа (авторизация).

Аудит и мониторинг: отслеживание и анализ действий пользователей и систем для выявления несанкционированных действий и инцидентов.

Защита от вредоносных программ: обеспечение защиты от вирусов, троянов, шпионского ПО и других вредоносных программ.

Физическая безопасность: защита физической инфраструктуры, такой как серверные центры и сетевое оборудование.

Социальная инженерия: обучение сотрудников организации и предотвращение атак, основанных на манипуляции сознанием людей.

Защита от DDoS-атак: предотвращение атак на доступность ресурсов путем перегрузки сети.

Шифрование: защита данных путем их шифрования, что делает их непонятными для неавторизованных лиц [1].

Информационная безопасность является важной для организаций, государственных учреждений и частных лиц, так как утечка и потеря конфиденциальных данных могут привести к серьезным последствиям, включая финансовые убытки и ущерб репутации. Многие организации имеют отдельные отделы по информационной безопасности и разрабатывают стратегии для защиты своей информации.

Представляет интерес такой компонент, как DDoS-атаки – когда злоумышленники пытаются перегрузить веб-ресурс или сеть, создавая огромное количество запросов. Защита от DDoS-атак включает в себя различные стратегии и технологии, направленные на предотвращение или смягчение воздействия этих атак. Это может включать в себя фильтрацию трафика, использование CDN (сетей доставки контента), анализ поведения пользователей и другие методы, чтобы обеспечить стабильную работу веб-ресурса [2].

Защита от DDoS-атак включает в себя различные методы и технологии, предназначенные для предотвращения или смягчения воздействия таких атак. Вот некоторые из основных методов защиты от DDoS-атак:

Фильтрация трафика: Один из наиболее распространенных методов защиты – это использование средств фильтрации трафика. Это может включать в себя IP-фильтрацию, блокировку известных злоумышленных IP-адресов и применение средств обнаружения аномального трафика.

Использование CDN (Content Delivery Network): CDN – это сети доставки контента, которые распределяют нагрузку между различными серверами и географическими точками присутствия. Они могут помочь уменьшить нагрузку на основной сервер и улучшить скорость доставки контента.

Балансировка нагрузки: Использование балансировки нагрузки позволяет равномерно распределять запросы между несколькими серверами, что делает DDoS-атаки менее эффективными.

Обнаружение и анализ аномального трафика: Системы обнаружения аномалий могут выявлять необычные и агрессивные попытки доступа к ресурсам и предпринимать меры по их блокированию.

Прокси-серверы: Прокси-серверы могут использоваться для фильтрации трафика и скрытия реального IP-адреса сервера.

Облачные решения: Некоторые облачные провайдеры предоставляют услуги защиты от DDoS-атак, где они могут обрабатывать атаки перед тем, как они достигнут вашего сервера.

Тестирование на прочность: Проведение регулярных тестов на прочность позволяет выявить уязвимости и улучшить систему защиты.

Важно понимать, что защита от DDoS-атак – это сложный и постоянно меняющийся процесс. Злоумышленники постоянно находят новые способы проведения атак, поэтому необходимо постоянно обновлять и улучшать методы защиты, чтобы обеспечить стабильную работу веб-ресурса [3].

Методы шифрования играют важную роль в обеспечении информационной безопасности. Шифрование используется для защиты конфиденциальности

данных и обеспечения их целостности, а также для обеспечения подлинности информации [1]. Вот несколько методов шифрования, которые широко применяются в современных системах информационной безопасности:

Симметричное шифрование: Этот метод использует один ключ как для шифрования, так и для расшифровки данных. Однако проблема симметричного шифрования заключается в том, что обе стороны обмена данными должны иметь доступ к ключу, что может создавать риски безопасности при передаче ключа.

Асимметричное шифрование: Этот метод использует пару ключей: открытый и закрытый. Открытый ключ используется для шифрования данных, а закрытый ключ – для их расшифровки. Это устраняет риски безопасности, связанные с распространением ключей, что делает его более надежным в сравнении с симметричным шифрованием.

Хэширование: Этот метод используется для обеспечения целостности данных путем создания фиксированной длины хэш-суммы, которая представляет собой уникальную строку символов, созданную из входных данных. Любое незначительное изменение в исходных данных приведет к значительному изменению хэш-суммы, что делает его полезным для проверки целостности данных.

Протоколы обмена ключами: Эти протоколы используются для безопасного обмена ключами шифрования между сторонами, участвующими в коммуникации. Примеры таких протоколов включают протоколы Диффи-Хеллмана и RSA.

Шифрование на уровне файлов и дисков: Этот метод используется для защиты данных на уровне файлов и дисков, обеспечивая их конфиденциальность и целостность. Примеры включают BitLocker для Windows и FileVault для macOS.

Протоколы SSL/TLS: Эти протоколы используются для защиты данных при передаче через Интернет. Они обеспечивают шифрование данных между клиентом и сервером, защищая данные от перехвата злоумышленниками.

Важно выбирать соответствующий метод шифрования в зависимости от конкретных требований безопасности информации и учитывать возможные уязвимости и риски, связанные с каждым методом. Кроме того, рекомендуется

комбинировать различные методы шифрования для повышения общего уровня безопасности системы.

Список литературы

1. Гродзенский Я.С. Информационная безопасность / Я.С. Гродзенский. – М.: РГ-Пресс, 2023. – 144 с. – DOI 10.31085/9785998808456-2020-144. – EDN VWAYBT

2. Басканов А.Н. Способы противодействия и средства раннего выявления DDoS-атак / А.Н. Басканов // Экономика и качество систем связи. – 2019 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstva-rannego-vyyavleniya-ddos-atak (дата обращения: 24.10.2023). EDN RRAPSF

3. Титов Ф.М. Исследование методов защиты от атаки DDOS / Ф.М. Титов // Научные междисциплинарные исследования: сборник материалов II Международной научно-практической конференции (Саратов, 5 июня, 2020 г.). – М.: КДУ, 2020. – С. 36–41.